

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004 年 9 月 30 日 (30.09.2004)

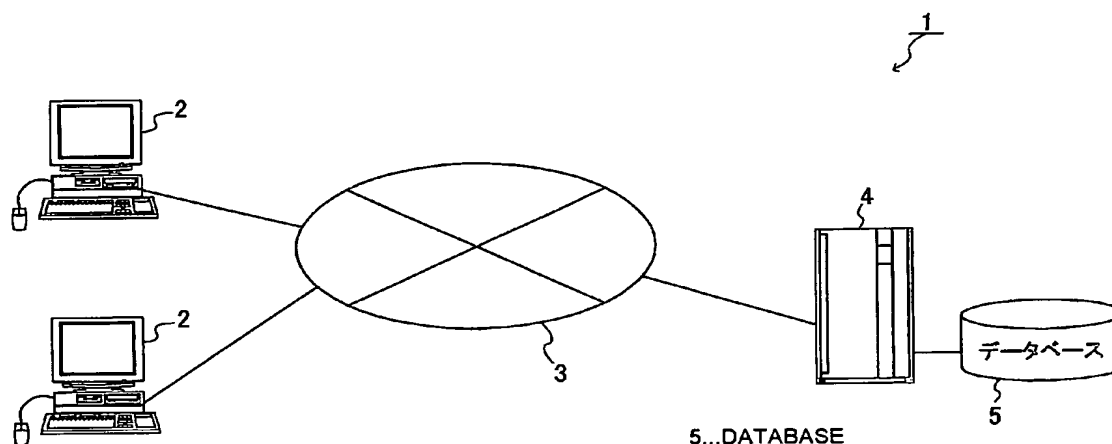
PCT

(10) 国際公開番号
WO 2004/084483 A1

- (51) 国際特許分類: H04L 9/08,
G09C 1/00, G06F 17/30, 17/60, 12/14
- (21) 国際出願番号: PCT/JP2003/003413
- (22) 国際出願日: 2003 年 3 月 20 日 (20.03.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 株式会社
日本医療データセンター (JAPAN MEDICAL DATA
CENTER CO., LTD.) [JP/JP]; 〒102-0083 東京都 千代
田区 麹町三丁目 1 番地 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 岡 博志 (OKA, Hi-
roshi) [JP/JP]; 〒164-0003 東京都 中野区 東中野二丁目
- 1 3 番 4 号 Tokyo (JP). 木村 真也 (KIMURA, Shinya)
[JP/JP]; 〒651-2275 兵庫県 神戸市西区 榎野台五丁目
2 番地 C-1407 Hyogo (JP).
- (74) 代理人: 黒田 健二, 外 (KURODA, Kenji et al.); 〒
105-0001 東京都 港区 虎ノ門 3 丁目 6 番 2 号 第 2 秋
山ビル 4 階・5 階 黒田特許事務所 Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB,
BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,
DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,
ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,
LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI,
NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK,
SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN,
YU, ZA, ZM, ZW.
- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ,
SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM,
[続葉有]

(54) Title: INFORMATION MANAGEMENT SYSTEM

(54) 発明の名称: 情報管理システム



(57) Abstract: An information management system for surely protecting personal information while securing informational availability in processing data including personal information. In an information management system (1), processing target data including the personal information are acquired by an information manager (2), and personal information is extracted from the processing target data and arithmetically operated with a unidirectional function on the basis of the extracted personal information to generate a unique code. The personal information included by the processing target data is substituted with the unique code to generate primary conversion data. This primary conversion data is transmitted from the information manager (2) to an information center unit (4) and stored in a database (5) and used for statistical processing.

(57) 要約: 個人情報を含むデータを処理する際に、情報の有用性を確保しながら個人情報を確実に保護することが可能な情報管理システムを提供する。情報管理システム (1) において、個人情報を含む処理対象のデータを情報管理装置 (2) によって取得し、処理対象のデータから個人情報を抽出し、抽出した個人情報をもとに、一方関数による演算を行ってユニークコードを生成する。そして、処理対象のデータに含まれる個人情報をユニークコードに置き換えることで、一次変換データを生成し、この一次変換データを情報管理装置 (2) から情報センタ装置 (4) に送信し、データベース (5) に格納して、統計的処理に用いる。



AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許
(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,
GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR),
OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

2 文字コード及び他の略語については、定期発行される
各 *PCT* ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

明 細 書

情報管理システム

5 技術分野

本発明は、個人情報を含む情報を管理する情報管理システムに関する。

背景技術

10 情報化の進展により、政府機関、民間企業、公益団体等においては、電子化された大量の情報が取り扱われるようになった。電子化された情報は、蓄積、検索、複製等の処理を簡単に行うことができ、さらに詳細な分析を行うなどの高度なデータ処理を行えるため、有用性が高い。

ところで、上記電子化された情報は、個人の氏名、生年月日、住所、電話番号、性別、家族構成等の個人情報を含むことが少なくない。個人情報は、悪用やプ
15 ライバシーの侵害を防止するために慎重に取り扱われなければならない、必要に応じて隠蔽する必要がある。

しかし、例えば個人の属性に関する情報を統計的に処理する場合、個人情報を含む情報を大量に収集せざるを得ないので、嚴重に情報管理を行うために多大な
20 労力が費やされる。そこで、個人情報を効率よく確実に保護する方法が、種々検討されていた。

例えば、個人情報を示す文字列を、全て無意味な文字や記号に置き換える方法があった。しかしこの方法では、個人情報が完全に失われてしまうため、例えば、
一人の人物に関する複数の情報と、複数の人物に関する複数の情報との見分けが
25 つかなくなってしまうといった問題が生じる。この問題により、統計的処理に際して母集団の数が曖昧となり分析の精度が低下するなど、不都合を生じる恐れがあった。

そこで、個人情報を示す文字列の一部のみに、文字の並べ替えや他の文字への置き換え等の単純な操作を施す方法があった。この方法では、個人情報の一部が
もとの状態を保つので、例えば操作後の複数の個人情報を参照して、同一人物に

関する情報か別人に関する情報かを判別することは、一応可能である。しかし、この方法では、操作後の個人情報进行分析することで規則性が見いだされ、いかなる操作が行われたのかが判明してしまう可能性があった。このため、個人の健康状態や資産に関する情報等の嚴重に管理すべき情報を取り扱う場合には、セキュリティ上の懸念から、上記の方法を使うことはできなかった。

このように、個人情報を隠蔽するために、処理対象の個人情報に操作を施す場合、操作が複雑だと情報の有用性を損なってしまい、操作が単純だと個人情報を確実に保護することができないという問題があった。

そこで、個人情報を含む情報をパスワードを用いて暗号化する方法が採用されていた。しかしこの方法では、パスワードを、消失や漏洩が無いように管理しなければならず、管理負担が大きいという問題があった。また、多くの情報を暗号化して保管し、利用時に復号するといった方法では、情報を暗号化および復号する手間がかかり、情報処理の効率が低くなるという問題があった。

15 発明の開示

本発明は、個人情報を含む情報を処理する際に、情報の有用性を損なうことなく、個人情報を確実に保護することが可能な情報管理システムを提供することを目的とする。

上記の目的を達成するため、第1の発明は、

個人情報を含むデータを処理する情報管理装置であって、処理対象のデータから個人情報を抽出する個人情報抽出手段と、前記個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するユニークコード生成手段と、前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成する一次変換データ生成手段とを備えたことを特徴とする。

第2の発明は、第1の発明の情報管理装置において、前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータとを対応づけて記憶する記憶手段をさらに備えることを特徴とする。

第3の発明は、第1の発明の情報管理装置において、前記ユニークコード生成

手段は、前記個人情報抽出手段により抽出された個人情報から基準文字列を生成する基準文字列生成手段と、前記基準文字列をキーとして、所定の演算対象文字列を前記一方向関数により演算することによって、前記ユニークコードを生成する演算手段とを備えて構成されることを特徴とする。

5 第4の発明は、第3の発明の情報管理装置において、前記演算手段は、前記基準文字列に基づいて演算桁数を決定する桁数決定手段と、前記演算桁数を有する演算対象文字列を生成する演算対象文字列生成手段と、前記基準文字列をキーとして前記演算対象文字列を前記一方向関数により演算する演算実行手段とを備えて構成されることを特徴とする。

10 第5の発明は、第1の発明の情報管理装置において、前記一次変換データを暗号化して二次変換データを生成する二次変換データ生成手段と、前記二次変換データを他の装置へ出力する出力手段と、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理
15 対象のデータと、前記出力手段による出力記録とを対応づけて記憶する記憶手段と、をさらに備えることを特徴とする。

第6の発明は、個人情報を含むデータを処理する情報管理装置と、前記情報管理装置により処理されたデータを管理する情報センタ装置とが通信回線を介して接続されてなる情報管理システムであって、前記情報管理装置は、処理対象のデータから個人情報を抽出する個人情報抽出手段と、前記個人情報抽出手段により
20 抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するユニークコード生成手段と、前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成する一次変換データ生成手段と、前記一次変換データを暗号化して二次変換データを生成する二次変換データ
25 生成手段と、前記二次変換データを、前記通信回線を介して前記情報管理装置に出力する出力手段と、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力の記録とを対応づけて記憶する記憶手段とを備え、前記情

報センタ装置は、前記情報管理装置から送信された二次変換データを受信する受信手段と、前記受信手段により受信された二次変換データを復号して前記一次変換データを生成する復号手段とを備えることを特徴とする。

第 7 の発明は、第 6 の発明の情報管理システムにおいて、前記情報センタ装置
5 は、前記復号手段により生成された一次変換データを格納するデータ格納手段をさらに備え、前記データ格納手段に格納されたデータを、前記ユニークコードをキーとして処理することを特徴とする。

第 8 の発明は、第 7 の発明の情報管理システムにおいて、前記情報センタ装置
10 は、前記データ格納手段に格納された、前記ユニークコードを含む複数のデータの中から、同一のユニークコードを含むデータを検出することを特徴とする。

第 9 の発明は、個人情報を含むデータを処理する情報管理用コンピュータに、
個人情報抽出手段によって処理対象のデータから個人情報を抽出するステップと、
ユニークコード生成手段によって前記個人情報抽出手段により抽出された個人情報
をもとに一方向関数を用いた演算を行ってユニークコードを生成するステップ
15 と、一次変換データ生成手段によって前記処理対象のデータ中の個人情報を前記
ユニークコードに置き換えて一次変換データを生成するステップとを含む処理を
実行させるためのプログラムである。

第 10 の発明は、第 9 の発明のプログラムであって、前記情報管理用コンピ
ュータに、前記一次変換データと、前記一次変換データのもとになった前記処理対
20 象のデータとを対応づけて記憶手段に記憶するステップをさらに含む処理を実行
させることを特徴とする。

第 11 の発明は、第 9 の発明のプログラムであって、前記ユニークコード生成
手段によりユニークコードを生成するステップは、前記個人情報抽出手段により
抽出された個人情報から基準文字列生成手段によって基準文字列を生成するステ
25 ップと、演算手段によって、前記基準文字列をキーとして所定の演算対象文字列
を前記一方向関数により演算することにより前記ユニークコードを生成するステ
ップとからなることを特徴とする。

第 12 の発明は、第 11 の発明のプログラムであって、前記演算手段によって
前記ユニークコードを生成するステップは、桁数決定手段によって前記基準文字

列に基づいて演算桁数を決定するステップと、演算対象文字列生成手段によって前記演算桁数を有する演算対象文字列を生成するステップと、演算実行手段により前記基準文字列をキーとして前記演算対象文字列を前記一方向関数により演算するステップとからなることを特徴とする。

- 5 第13の発明は、第9の発明のプログラムであって、前記情報管理用コンピュータに、二次変換データ生成手段によって前記一次変換データを暗号化して二次変換データを生成するステップと、出力手段によって前記二次変換データを他の装置へ出力するステップと、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった
- 10 前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力記録とを対応づけて記憶手段に記憶するステップとをさらに含む処理を実行させることを特徴とする。

図面の簡単な説明

- 15 第1図は、本発明の実施の形態における処理の概念を示す図である。
- 第2図は、本発明の実施の形態の情報管理システムの構成を示す図である。
- 第3図は、第2図に示す情報管理装置の機能的構成を示すブロック図である。
- 第4図は、本発明の実施の形態において処理されるレセプトデータの構成を示す図である。
- 20 第5図は、第2図に示す情報管理システムの動作を示すフローチャートである。
- 第6図は、本発明の実施の形態におけるユニークコード生成処理を詳細に示すフローチャートである。
- 第7図は、本発明の実施の形態におけるユニークコード生成処理を具体的な例を挙げて説明する図である。
- 25 第8図は、本発明の実施の形態におけるユニークコード生成処理を、別の具体的な例を挙げて説明する図である。
- 第9図は、本発明の実施の形態におけるデータ送受信処理を詳細に示すフローチャートである。
- 第10図は、個人情報を含むデータを格納したデータベースの例を示す図であ

る。

第11図は、ユニークコードを含むデータを格納したデータベースの例を示す図である。

5 発明を実施するための最良の形態

第1図は、本発明の実施の形態の基本的概念を示す図である。本発明は、個人情報を含むデータを処理対象とする。

ここで、個人情報とは、それ自体または他の情報と組み合わせることにより個人を特定することが可能な情報、及び、個人の履歴（学歴、職歴および個人の行動履歴を示すその他の情報を含む）、各種組織における個人の属性を示す情報等、本人の承諾を得なければ利用や公開ができない、あるいは秘匿することが好ましいとされる情報である。個人情報の具体例としては、氏名、生年月日、性別、年齢、住所、連絡先（電話番号、ファクシミリ番号、電子メールアドレス等）、社会保障や税金に係る情報（社会保障番号、納税者番号等）、職業に関する情報（勤務先の名称、所在地、連絡先、所属部門、職責等）、在籍中または卒業した教育機関に関する情報（教育機関の名称、所在地、連絡先、入学または卒業年度、学籍番号等）、個人の購買履歴を示す情報（商品購入履歴、個人が加入する生命保険や損害保険の証券番号等）、クレジットカード番号等の個人の与信情報、金融機関の口座番号等が挙げられる。

第1図に示す基本データ101は、第三者が識別可能な状態で個人情報102を含む。本実施の形態では、個人情報102をもとにユニークコード104を生成し、個人情報102をユニークコード104に置き換えることで一次変換データ103を生成する。つまり、一次変換データ103は、基本データ101の個人情報102をユニークコード104に置き換えた以外は、基本データ101と同一のデータである。

さらに、本実施の形態では、一次変換データ103を他の装置へ出力する場合、すなわち通信回線を介して送受信し、或いは記録媒体等に記録して輸送する場合に、一次変換データ103全体を所定のパスワードで暗号化した二次変換データ105を用いる。二次変換データ105の出力を受けた装置においては、上記パ

スワードを用いて二次変換データ 105 を復号すれば、一次変換データ 103 を得ることができる。

以下、本実施の形態の好ましい具体的態様について、第 2 図～第 11 図の各図を参照して詳細に説明する。

- 5 第 2 図は、本発明の実施の形態の情報管理システムの構成を示す図である。第 2 図に示す情報管理システム 1 は、情報管理装置 2 と、ネットワーク 3 を介して情報管理装置 2 に接続された情報センタ装置 4 とから構成される。なお、第 2 図には 2 台の情報管理装置 2 を示したが、情報管理装置 2 の数は 1 以上であれば良い。
- 10 ネットワーク 3 は、専用線、公衆電話回線、衛星通信回線等の各種通信回線を含んで構成される。なお、ネットワーク 3 は、インターネットのようなオープンなネットワークであっても良いし、限られた装置のみアクセス可能なクローズドネットワークであっても良い。また、ネットワーク 3 の具体的態様（回線の種類、帯域幅、ネットワークトポロジ、使用するプロトコル）については特に限定され
- 15 ず、各種のサーバ装置やファイアーウォール装置、ゲートウェイ装置等を含むものとしても良い。

情報管理装置 2 および情報センタ装置 4 は、ネットワーク 3 を介して、互いに各種データや制御情報等を送受信する。

- 20 情報センタ装置 4 は、情報管理装置 2 から送信される情報を受信し、受信した情報が暗号化されている場合は復号する。さらに、情報センタ装置 4 はデータベース 5 を備え、復号した情報をデータベース 5 に蓄積させるとともに、データベース 5 に蓄積された情報を検索し、選択（selection）、射影（projection）、結合（join）等の操作を実行する。

- 25 第 3 図は、情報管理装置 2 の機能的構成を示すブロック図である。第 3 図に示すように、情報管理装置 2 は、CPU（Central Processing Unit）21、RAM（Random Access Memory）22、記憶装置 23、記録媒体読取装置 24、入力装置 25、表示装置 26、および通信制御装置 27 を備え、これらの各部はバス 28 に接続されている。

CPU 21は、入力装置25を用いてユーザが入力した指示に基づいて、記憶装置23に格納されたコンピュータプログラムを読み出して実行し、第5図に示す処理を実行する。すなわち、CPU 21は、記録媒体読取装置24によって記録媒体に記録された情報を読み取ることにより基本データを取得し、基本データから一次変換データを生成する。さらに、CPU 21は、一次変換データを暗号化して二次変換データを生成し、ネットワーク3を介して情報センタ装置4に送信する。

RAM 22は、CPU 21によって実行されるコンピュータプログラムや、コンピュータプログラムの実行時に処理されるデータを一時的に格納する。

記憶装置23は、CPU 21によって実行されるコンピュータプログラムや、コンピュータプログラムの実行時に処理されるデータを、CPU 21による読み取りが可能な状態で記憶している。記憶装置23は、CPU 21からの読み出し要求に応じて、要求されたコンピュータプログラムやデータ等をCPU 21に出力する。また、記憶装置23は、CPU 21からの書き込み要求に応じてデータを記憶する。

記録媒体読取装置24は、磁氣的、光学的記録媒体や半導体メモリ素子を内蔵した記録媒体等、可搬型の記録媒体に記録された情報を、CPU 21の制御に従って読み取る装置である。

入力装置25は、マウス、ペンタブレット、タッチパネル、ディジタイザ等のポインティングデバイス、及び、キーボード等の入力デバイスを備え、上記入力デバイスの操作に応じて操作信号を生成し、CPU 21に出力する。

表示装置26は、CRT (Cathode Ray Tube) やLCD (Liquid Crystal Display) 等の表示画面を有し、入力装置25により入力された指示やCPU 21により実行された処理の結果等を上記表示画面上に表示する。

通信制御装置27はネットワーク3に接続され、ネットワーク3を介して各種情報を送受信する。

第4図は、本実施の形態において処理対象となるレセプトデータの構成を示す図である。第4図(a)は、レセプトデータ全体の構成を示し、第4図(b)は特に個人情報を含む部分の構成を示す図である。情報管理システム1は様々なデ

ータを処理することが可能であるが、本実施の形態では、個人情報を含むデータ
の一例としてレセプトデータを処理する場合について説明する。

ここで、レセプトとは、正式には診療報酬明細書といい、日本国内の医療保険
制度を利用して診療報酬の支払いを受けるために、医療機関が作成して保険者に
5 提出する書類である。レセプトには、患者自身の個人情報、患者が診療を受けた
医療機関に関する情報、診療内容を示す情報、診療報酬金額に関する情報等、様
々な情報が記録される。

レセプトを用いた診療報酬の請求は、通常、月ごとに行われるので、医療機関
は、一人の患者に対して一ヶ月間に行った診療行為の診療報酬を、一通のレセプ
10 トにより請求する。一人の患者が複数の医療機関で診療を受けた場合、これら複
数の医療機関は、それぞれレセプトを作成して提出する。従って、一人の患者に
ついて、ひと月に複数のレセプトが提出されることがある。

診療に関する情報を電子化して処理している医療機関では、レセプトに記録す
る情報をまとめたレセプトデータを作成し、指定された書式でレセプトデータを
15 印刷することでレセプトを作成している。

レセプトデータは、例えば、第4図（a）に示すように構成される。なお、第
4図（a）はあくまで一例を示す図であり、必ずしも全てのレセプトが第4図（
a）のように構成されるとは限らない。

レセプトデータ6は、レセプトに記録すべき各種の情報をC S V（Comma
20 Separated Value）形式で記述したものであり、医療機関レコード61、レセプ
ト共通レコード62、保険者レコード63、老人レコード64、公費レコード6
5、傷病名レコード66および摘要情報67を含んで構成される。

医療機関レコード61は、患者が診療を受けた医療機関、すなわちレセプトを
作成する医療機関に関する情報およびその他の情報を含む最大62バイトのデー
25 タで構成される。具体的には、医療機関レコード61は、医療機関の所在地が属
する自治体、医療機関に付与されたコード、医療機関の名称、診療科目、診療報
酬を請求する年月等を示す情報を含む。

レセプト共通レコード62は、主として患者に関する情報を含む最大122バ
イトのデータで構成される。レセプト共通レコード62は、具体的には、患者が

診療を受けた年月、患者の氏名、生年月日、性別、診療報酬のうち患者が自己負担すべき割合、カルテの番号等の情報を含み、患者が入院治療を受けた場合は、入院年月日、入院した病棟の種別、病床数等の情報を含む。

5 保険者レコード 6 3 は、診療報酬の請求先の保険者に関する情報や、患者の医療保険加入者番号、診療報酬金額および内訳に関する情報等を含む最大 1 3 8 バイトのデータで構成される。

老人レコード 6 4 は、老人医療費制度に基づいて自治体による医療費の給付を受けるために必要な各種情報を含み、最大 1 4 3 バイトのデータで構成される。

10 公費レコード 6 5 は、特例的な医療費の公的補助を受けるために必要な各種情報を含み、最大 6 3 バイトのデータで構成される。

傷病名レコード 6 6 は、患者の傷病に関する情報を含む最大 1 3 9 バイトのデータで構成される。

15 摘要情報 6 7 は、医療機関が患者に対して行った診療行為の内容等を示す情報を含む診療行為レコード（最大 3 2 バイト）、使用した医薬品に関する情報を含む医薬品レコード（最大 3 3 バイト）、使用した機材に関する情報を含む特定機材レコード（最大 8 6 バイト）、及び、診療内容に関する追加的な情報であるコメント等の情報を含むコメントレコード（最大 9 0 バイト）を含む最大 2 4 1 バイトのデータで構成される。

20 レセプト共通レコード 6 2 は、第 4 図（b）に示すように、患者の個人情報である氏名 6 2 1（最大 4 0 バイト）、生年月日 6 2 2（7 バイト）および性別コード 6 2 3（1 バイト）を含む。性別コードは、性別を示すコードとして予め定められたものである。本実施の形態では、男性を「1」、女性を「2」で表す。

続いて、情報管理システム 1 の動作について説明する。

25 第 5 図は、第 2 図に示す情報管理システムの動作を示すフローチャートである。第 5 図（a）は、特に情報管理装置 2 の動作を示し、第 5 図（b）は情報センタ装置 4 の動作を示す。

ステップ S 1 1（第 5 図（a））で、情報管理装置 2 は、記録媒体読取装置 2 4 によって記録媒体から情報を読み取ることにより、処理対象の基本データ（レセプトデータ）を取得する。

ステップS 1 2で、情報管理装置2は基本データ中の個人情報を検出する。次に、ステップS 1 3で、情報管理装置2は、ステップS 1 2で検出した個人情報をもとにユニークコードを生成する処理を実行する。ステップS 1 3のユニークコード生成処理については、第6図を参照して後で説明する。

5 ユニークコード生成処理の後、ステップS 1 4で、情報管理装置2は、基本データを複製し、複製した基本データ中の個人情報をユニークコードに置き換えることによって一次変換データを生成する。ステップS 1 5で、情報管理装置2は、ステップS 1 4で生成した一次変換データを基本データとともに記憶装置23に記憶し、ステップS 1 6に移行して、入力装置25からの指示入力を受け付ける。

10 ステップS 1 6で、入力装置25から、情報センタ装置4にデータを送信する旨の指示が入力された場合、情報管理装置2はステップS 1 7に移行し、情報センタ装置4へデータを送信する処理を実行する。ステップS 1 7のデータ送受信処理については、第9図(a)を参照して後で説明する。

ステップS 1 7のデータ送受信処理の後、情報管理装置2は動作を終了する。

15 また、ステップS 1 6において、入力装置25から指示が入力されなかった場合、情報管理装置2はステップS 1 1に戻る。

情報センタ装置4は、情報管理装置2がステップS 1 7のデータ送受信処理を開始すると同時に、ステップS 2 1(第5図(b))に移行してデータ送受信処理を実行する。ステップS 2 1のデータ送受信処理については、第9図(b)を
20 参照して後で説明する。

データ送受信処理の後、情報センタ装置4はステップS 2 2に移行し、ステップS 2 1で受信した情報について、ユニークコードをキーとして、データベースを操作する処理を行う。

第6図は、第5図(a)のステップS 1 3に示すユニークコード生成処理を、
25 より詳細に示すフローチャートである。

ステップS 3 1で、情報管理装置2は基本データから個人情報を抽出する。ステップS 3 2で、情報管理装置2は、抽出した個人情報から半角スペースおよび全角スペースを除去して基準文字列を作成する。

続くステップS 3 3で、情報管理装置2は、基準文字列を構成する全ての文字

について、文字コードを取得する。なお、ステップS 3 3においては、A S C I Iコード、U n i c o d e、J I Sコード、シフトJ I Sコード等の文字コードセット等の各種文字コードセットを使用することが可能である。

5 ステップS 3 4で、情報管理装置2は、基準文字列を構成する全ての文字の文字コードを合計する。続くステップS 3 5で、情報管理装置2は、ステップS 3 4で求めた文字コードの和を3 2で除算し、商と余りを求める。情報管理装置2はステップS 3 6に移行し、求めた余りに1 0 0を加えて演算桁数とする。

10 以上のステップS 3 3～ステップS 3 6の処理によって、演算桁数は、1 0 0～1 3 1のいずれかに決定される。なお、演算桁数がとりうる値の範囲は、ステップS 3 5で用いる除数（法）を変化させることによって決定される。例えば、除数（法）を5 0とすれば、1 0 0～1 4 9の範囲で演算桁数が決定される。また、例えば除数（法）を1 0とすれば1 0 0～1 0 9の範囲で演算桁数が決定される。つまり、除数（法）を整数 n とすれば、演算桁数は $1 0 0 \sim \{1 0 0 + (n - 1)\}$ の範囲で決定される。本実施の形態ではあくまで一例として、除数（法）に3 2を用いている。

その後、情報管理装置2はステップS 3 7に移行して、演算桁数と同じ桁数を有する文字列を生成し、N U L Lクリアする。これにより、演算桁数に等しい桁数を有し、かつ、全ての桁が「0（ゼロ）」である文字列が生成される。このステップS 3 7で生成された文字列を演算対象文字列とする。

20 ステップS 3 8で、情報管理装置2は、演算対象文字列を、一方向ハッシュ関数によって、基準文字列をキーとして演算する。ステップS 3 8の演算が完了した後、情報管理装置2はステップS 3 9に移行し、演算結果をバイナリダンプして文字列を生成し、生成した文字列をユニークコードとする。ステップS 3 9でバイナリダンプを行うのは、ハッシュ関数を用いた演算の結果が制御コードを含む可能性があるためである。

25 第6図に示すユニークコード生成処理では、個人情報からスペースを除いた基準文字列の文字コードをもとに演算桁数が決定されるので、基準文字列が一文字でも異なる場合は、演算桁数が異なる。一般に、ハッシュ関数を用いた演算では、初期値の変化によって演算結果が極めて大きな影響を受けることが明らかになっ

ている。従って、演算桁数がわずかでも異なる場合、演算結果は極端に異なったものとなる。さらに、第6図に示すユニークコード生成処理では、基準文字列をキーとして演算を行うので、基準文字列が一文字でも異なっていると、演算結果に、さらに大きな差を生じる。

- 5 例えば、氏名、生年月日および性別をもとにユニークコードを生成する場合、氏名、生年月日、性別のいずれか一つの情報が、一文字だけでも違っていれば、全く異なるユニークコードが生成されるのである。従って、異なる複数の人物の個人情報から同一のユニークコードが生成される確率はゼロに近く、無視できる。

10 また、このように生成されたユニークコードは、それ自体は一見して無意味な文字列にしか見えないので、多数のユニークコードを分析しても何ら規則性を発見することはできない。このため、ユニークコードを演算して個人情報を得ることは実質的に不可能であり、そのユニークコードが、氏名のみを基準文字列として生成されたのか、氏名と生年月日を含む基準文字列から生成されたのかを判別することも不可能である。

- 15 このように、ユニークコードは、個人情報をもとに生成されるにも関わらず、ユニークコード自体から個人情報を知る手段がないので、一次変換データのみを利用する限りにおいて、個人情報が漏洩する恐れはない。

20 さらに、第6図に示す処理においては、個人情報からスペースを除去した後にユニークコードを生成するので、スペースの使い方等の表記方法の違いにも対応することができる。なお、第6図のステップS32では全角および半角のスペースを除去するものとしたが、例えば、個人情報中にアルファベットの大文字と小文字とが混在する場合に、全てのアルファベットを小文字に変換する処理を行っても良い。

- 25 さらに、同一人物の個人情報から、意図的に異なる複数のユニークコードを生成することも可能である。すなわち、氏名と生年月日のみを基準文字列とした場合のユニークコードと、氏名、生年月日および性別を基準文字列とした場合のユニークコードは異なるものになる。このため、特定の個人について、個人情報とこの個人情報をもとに生成したユニークコードとの対応関係が漏洩してしまった場合は、基準文字列の内容を変えて新たなユニークコードを生成すれば、それ以

上の個人情報の漏洩を防ぐことができる。また、基本データの形態やユニークコードの用途に応じて、適宜、異なるユニークコードを生成することにより、ユニークコード生成処理の処理速度を高めることも、ユニークコードをさらに複雑化することも可能であり、効率よくユニークコードを利用することができる。

- 5 第7図は、第6図に示すユニークコード生成処理を、具体的な例を挙げて説明する図である。第7図の例では、1970年5月15日生まれの山田太郎という男性の個人情報からユニークコードを生成する。

情報管理装置2によって抽出される個人情報は、氏名「山田 太郎」、生年月日「19700515」および性別コード「1」である。情報管理装置2によって半角および全角のスペースが除去されると、基準文字列「山田太郎197005151」が作成される。基準文字列には漢字4文字で構成される日本語の人名が含まれるので、
10 情報管理装置2は、シフトJIS文字コードセット等の日本語用文字コードセットを用いて文字コードを取得する。日本語用文字コードセットでは漢字は2バイト文字として扱われるので、4文字の漢字から各々2バイトの文字コードが得られる。また、上記日本語用文字コードセットでは半角数字は1バイト文字として
15 扱われるので、「197005151」の9文字から各々1バイトの文字コードが得られる。これにより、基準文字列「山田太郎197005151」から17バイトの文字コードが得られる。

次に、情報管理装置2によって、基準文字列の文字コードが合計される。第7
20 図に示すように「 $8E+52+93+63+91+BE+98+59+31+39+37+30+30+35+31+35+31=5E3$ (16進数表記)」の演算が情報管理装置2によって行われ、文字コードの和「5E3」が求められる。「5E3」は10進数で表記すると「1507」である。続いて、情報管理装置2によって、文字コードの和「1507」が「32」で除算され、商が「47」、余りが「3」と求められる。演算桁数は、余りの「3」に「100」を加えて1
25 03桁に決定される。その後、情報管理装置2によって全ての桁が「0(ゼロ)」で構成される103桁の演算対象文字列が生成され、基準文字列「山田太郎197005151」をキーとしてハッシュ関数による演算が行われる。演算結果はバイナリダンプされ、例えば、ユニークコード「69654665019b733fe725353a5884fd94469d85e857820ad6742c3fc1b1b2elec3ee38c2e63b541c7b11f0781cda5a82838b0d5e5b3

2eceffffe6bd484356b69c97498dbdf54e706719ecc7d90db8254762b4437b429fb61843c009b1b9f5ec3d7b6085b5548b1」が生成される。なお、このユニークコードは、セキュリティ上の配慮から、実際に上記基準文字列をもとに得られるユニークコードの一部を改変したものである。

- 5 第8図は、第6図に示すユニークコード生成処理を、別の具体的な例を挙げて説明する図である。第8図の例では、1970年2月26日生まれのNancy Lopezという女性の個人情報からユニークコードを生成する。

情報管理装置2によって抽出される個人情報は、氏名「Nancy Lopez」、生年月日「19700226」および性別コード「2」である。情報管理装置2によって半角および全角のスペースが除去されると、基準文字列「NancyLopez197002262」が作成される。半角の英数字は、各種文字コードセットにおいて1バイト文字として扱われるので、基準文字列「NancyLopez197002262」からは、19バイトの文字コードが得られる。

次に、情報管理装置2によって、基準文字列の文字コードが合計される。第8図に示すように「4E+61+6E+63+79+52+6F+70+65+7A+31+39+37+30+30+32+32+36+32=5DB(16進数表記)の演算が情報管理装置2によって行われ、文字コードの和「5DB」が求められる。「5DB」は10進数で表記すると「1499」である。続いて、情報管理装置2によって、文字コードの和「1499」が「32」で除算され、商が「46」、余りが「27」と求められる。演算桁数は、余りの「27」に「100」を加えて127桁に決定される。その後、情報管理装置2によって全ての桁が「0(ゼロ)」で構成される127桁の演算対象文字列が生成され、基準文字列「NancyLopez197002262」をキーとしてハッシュ関数による演算が行われる。演算結果はバイナリダンプされ、例えば、ユニークコード「56b03813bad4c752a5c13247a0bc194ca607caf2e295646a061027d09c00d9ec9767f6e825c521647b16a19df9ee6041ae400b7fa1026c93491d1d577a815129626493b6e9da791e85203fd00018e6022a0215afb571b67fffd47d3e687dad79252ad98012bdd73d476edc0639a73cd9ca2a7f3c831e065bdd」が生成される。なお、このユニークコードは、セキュリティ上の配慮から、実際に上記基準文字列をもとに得られるユニークコードの一部を改変したものである。

第9図は、本発明の実施の形態のデータ送受信処理をより詳細に示すフローチ

ャートである。第9図(a)は第5図(a)のステップS17で情報管理装置2が実行する処理を示し、第9図(b)は第5図(b)のステップS21で情報センタ装置4が実行する処理を示す。

この第9図に示すデータ送受信処理では、DH (Diffie-Hellman) 方式による
5 公開鍵の交換を行って、一次変換データを送受信する。

ステップS41 (第9図(a)) で、情報管理装置2は、例えば乱数を用いて秘密鍵PR1を生成する。ステップS42で、情報管理装置2は、所定の演算式を用いて秘密鍵PR1から公開鍵PU1を生成する。そして、ステップS43で、
10 情報管理装置2は、公開鍵PU1をネットワーク3を介して情報センタ装置4に送信するとともに、情報センタ装置4から送信される公開鍵PU2を受信する。

一方、情報センタ装置4は、ステップS51 (第9図(b)) で秘密鍵PR2を、例えば乱数を用いて生成し、ステップS52で、所定の演算式を用いて秘密鍵PR2から公開鍵PU2を生成する。そして、情報センタ装置4は、ステップS53で、公開鍵PU2をネットワーク3を介して情報管理装置2に送信すると
15 ともに、情報管理装置2から送信される公開鍵PU1を受信する。

以上のステップS41～S43及びステップS51～S53の処理により、情報管理装置2と情報センタ装置4とは、自己が生成した秘密鍵と、相手が生成した公開鍵とを保持することになる。なお、情報管理装置2と情報センタ装置4との間で、以上のステップS41～S43及びステップS51～S53の処理を行
20 っておいてから、第5図に示す処理を行っても良い。すなわち、第5図の処理を行うに先立って、予め、情報管理装置2と情報センタ装置4とが、自己が生成した秘密鍵と相手が生成した公開鍵とを保持している構成としても良い。この場合、公開鍵PU1および公開鍵PU2は、ネットワーク3を介して送受信しても良いし、入力装置25等による入力操作や可搬型の記録媒体を用いて、情報管理装置
25 2及び情報センタ装置4に入力されても良い。

ステップS44 (第9図(a)) で、情報管理装置2は、自己が生成した秘密鍵PR1と情報センタ装置4から受信した公開鍵PU2とをもとに、共通鍵CKを生成する。

ステップS45で、情報管理装置2は、セッション鍵SKを生成する。続くス

ステップS 4 6で、情報管理装置2は、セッション鍵SKを用いて一次変換データを暗号化することにより、二次変換データを生成する。

さらに、情報管理装置2はステップS 4 7に移行して、セッション鍵SKを共通鍵CKによって暗号化し、ステップS 4 8で、暗号化したセッション鍵SKを

5 二次変換データに付加して情報センタ装置4へ送信する。

その後、ステップS 4 9で、情報管理装置2は、情報センタ装置4への送信結果を示す送信ログを作成して、二次変換データと送信ログを、記憶装置23に記憶された基本データおよび一次変換データに対応づけて記憶装置23に記憶し、処理を終了する。

10 一方、情報センタ装置4は、ステップS 5 5（第9図（b））で、暗号化されたセッション鍵SKと二次変換データとを受信する。続くステップS 5 6で、情報センタ装置4は、受信したセッション鍵SKを、ステップS 5 4で生成した共通鍵CKにより復号し、ステップS 5 7で、復号したセッション鍵SKにより二次変換データを復号して一次変換データを得る。

15 ステップS 5 8で、情報センタ装置4は、ステップS 5 7で得られた一次変換データをデータベース5に登録し、処理を終了する。

第10図は、個人情報を含むデータを格納したデータベースの例を示す図である。第10図に例示するデータベースは、個人の氏名、生年月日、性別コード、医療機関名、傷病名、診療日数、診療内容の各項目のデータを含むレコードを格納するものであって、複数の個人に関する複数のレコードを格納している。

20 このように、個人情報を含むデータをデータベース化すると、個人情報をキーとして、選択、射影、結合等のデータベース操作を行い、個人毎にデータを抽出することが可能である。しかしながら、個人情報を格納したデータベースは個人情報の保護のための方策を施す必要がある。

25 そこで、第10図に示すデータベースに格納されるレコードを、個人情報の代わりにユニークコードを含む一次変換データに置き換えた例を、第11図に示す。

第11図に例示するデータベースは、ユニークコードを含む複数のレコードを格納している。第11図に示すデータベースは個人情報を含まないため、個人情報を保護するための特別な方策は不要である。

さらに、第 11 図に示すデータベースにおいては、ユニークコードをキーとして、個人毎にデータを操作することが可能である。例えば、第 11 図に示すように、ユニークコード「548b1695d8e9a2b6085b5」をキーとして選択操作を行うと、No. 1 と No. 4 の二つのレコードが抽出される。抽出された二つのレコードは、ユニークコードが同一であることから同一人物に関するレコードであることがわかる。従って、第 10 図に示すデータベースを、第 11 図に示すデータベースに置き換えても、情報の検索容易性は損なわれない。

このように、本実施の形態では、個人情報ユニークコードに置き換えた一次変換データを用いることにより、情報の有用性を損なうことなく、個人情報を確実に保護することが可能である。

以上のように、本実施の形態における情報管理システム 1 によれば、個人情報を含む処理対象のデータをそのままデータベース化せず、処理対象のデータ（基本データ）中の個人情報からユニークコードを生成し、個人情報をユニークコードに置き換えた一次変換データを生成して、一次変換データをデータベース 5 に格納して統計的処理に用いる。ユニークコードは、個人情報からスペースを除去した基準文字列をもとに、一方向ハッシュ関数を用いた演算により生成されるので、逆の演算を行ってもとの個人情報を知ることがほぼ不可能である。このため、一次変換データを処理する過程において、個人情報が漏洩する心配が全くない。

また、一方向ハッシュ関数の、演算結果が初期値の変化に極端に影響されるという特徴により、基準文字列が異なる場合、すなわち別の個人情報を用いた場合には、必ずといっていいほど別の、著しく異なるユニークコードが生成される。つまり、別人の個人情報から同一のユニークコードが生成される可能性は極めて低く、無視できる程度であり、一次変換データの有用性を高いレベルで保つことができる。さらに、ユニークコードは、基準文字列をもとに演算桁数を決定し、この演算桁数の演算対象文字列を、基準文字列をキーとして演算することにより生成されるので、基準文字列が異なる場合には、著しく異なるユニークコードが生成されるので、別人の個人情報から同一のユニークコードが生成される可能性が一段と低くなり、一次変換データの有用性を、より一層高いレベルで保つことができる。

従って、ユニークコードは、個人情報と同様に、一人の個人に対して固有の値となるので、ユニークコードを含む多数のデータを、個人毎に検索、抽出する操作に利用することができる。このように、個人情報の代わりにユニークコードを含む一次変換データは、個人情報を含むデータと同等の有用性があり、統計的処理に活用できる。そして、この一次変換データを用いることにより、個人情報を含むデータを処理する際に、情報の有用性を損なうことなく、個人情報を確実に隠蔽して保護することができる。そして、情報管理システム 1 は、情報管理装置 2 によって、基本データから一次変換データを効率よく生成することができる。

また、情報管理装置 2 は、基本データから一次変換データを生成した場合には一次変換データと、もとになった基本データとを対応づけて記憶装置 2 3 に記憶する。さらに、一次変換データから二次変換データを生成して情報センタ装置 4 へ送信した場合には、二次変換データと、この二次変換データのもとになった一次変換データと、この一次変換データのもとになった基本データと、送信記録とを対応づけて記憶装置 2 3 に記憶するので、情報管理装置 2 における一次変換データの生成、二次変換データの生成および送信の履歴を示す情報を記憶することで、個人情報の流通管理を確実に行うことができる。

また、情報管理装置 2 から情報センタ装置 4 へ一次変換データを送信する際に、DH方式の鍵交換を行った上、一次変換データを暗号化して二次変換データを生成し、生成した二次変換データを、ネットワーク 3 を介して送信する。このため、ネットワーク 3 を介して情報を送信する間も、セキュリティ上の信頼性を確保することができる。さらに、万が一、一次変換データが第三者に漏洩しても、個人情報が知られる可能性は全く無いので、高い信頼性を確保できる。

さらに、情報センタ装置 4 は、情報管理装置 2 から受信した一次変換データをデータベース 5 に格納し、データベース 5 に格納された複数の一次変換データについて、ユニークコードをキーとして検索等の処理操作を行うことができ、例えば、同一のユニークコードを含む一次変換データを抽出する、いわゆる名寄せ処理を行うことも可能である。これにより、情報センタ装置 4 は、個人情報が漏洩する恐れが全く無い状態で、正確な統計的処理を実行することが可能となる。

なお、上記実施の形態においては、情報管理システム 1 の処理対象のデータと

してレセプトデータを用いる例について説明したが、本発明はこれに限定されるものではなく、例えば、金融機関の口座番号、口座名義人、預金残高や取引記録に関するデータを処理することも可能であるし、教育機関において生徒・学生の氏名と成績表とを含むデータを処理することも可能である。

- 5 また、上記実施の形態においては、情報管理装置 2 が基本データを取得する際に記録媒体読取装置 24 を用いる構成としたが、本発明はこれに限定されるものではなく、入力装置 25 からの入力によって、基本データを取得するようにしても良い。さらに、情報管理装置 2 を、記録媒体読取装置 24 に代えて可搬型の記録媒体に対し情報を書き込むことが可能な記録媒体読取／書込装置を備える構成とし、情報センタ装置 4 を、情報管理装置 2 によって情報が書き込まれた可搬型の記録媒体から情報を読み取るための読取装置を備える構成としても良い。この場合、情報管理装置 2 から情報センタ装置 4 へ二次変換データを送る際に、ネットワーク 3 を用いなくて、情報管理装置 2 の記録媒体読取／書込装置によって可搬型の記録媒体に二次変換データを書き込み、情報センタ装置 4 の読取装置によって、可搬型の記録媒体に書き込まれた二次変換データを読み取るといった方法を利用することができる。

その他の点においても、上記実施の形態の構成を適宜変更することは可能である。すなわち、上記実施の形態はあくまで一例であり、本発明の適用範囲を制限するものではない。

20

産業上の利用可能性

以上の説明から明らかなように、本発明によれば、以下に述べる効果が得られる。

- (1) 第 1 の発明によれば、個人情報を含むデータを処理する情報管理装置において、処理対象のデータから個人情報抽出手段によって個人情報を抽出し、ユニークコード生成手段により、個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成し、一次変換データ生成手段により、処理対象のデータ中の個人情報をユニークコードに置き換えて一次変換データを生成する。ここで生成されるユニークコードは、逆の演算を行っ

25

てもとの個人情報を知ることがほぼ不可能であり、かつ、異なる個人情報からは、必ずといっていいほど異なるユニークコードが生成される。従って、個人情報の代わりにユニークコードを含む一次変換データは、個人情報を含むデータと比較して同等の有用性があり、統計的処理に活用できる。そして、この一次変換データを
5 用いることにより、個人情報を含むデータを処理する際に、情報の有用性を損なうことなく、個人情報を確実に隠蔽して保護することができる。そして、第1の発明により、上記一次変換データを効率よく生成することができる。

(2) 第2の発明によれば、第1の発明の情報管理装置において、一次変換データと、この一次変換データのもとになった処理対象のデータとを対応づけて記憶
10 手段に記憶する。従って、情報管理装置において、個人情報を含む処理対象のデータと、ユニークコードを含む一次変換データとを保存しておくことができる。

(3) 第3の発明によれば、第1の発明の情報管理装置において、ユニークコード生成手段は、個人情報抽出手段により抽出された個人情報から基準文字列生成手段によって基準文字列を生成し、演算手段によって、基準文字列をキーとして、
15 所定の演算対象文字列を一方向関数により演算することによって、ユニークコードを生成する。これにより、基準文字列が異なる場合、すなわち別の個人情報を
用いた場合には、必ずといっていいほど別のユニークコードが生成される。つまり、別人の個人情報から同一のユニークコードが生成される可能性は無視できる
程度であり、一次変換データの有用性を高いレベルで保つことができる。

(4) 第4の発明によれば、第3の発明の情報管理装置において、演算手段は、
20 桁数決定手段によって基準文字列に基づいて演算桁数を決定し、演算対象文字列生成手段によって演算桁数を有する演算対象文字列を生成し、演算実行手段によ
って、基準文字列をキーとして演算対象文字列を一方向関数により演算する。こ
れにより、基準文字列が異なる場合には、著しく異なるユニークコードが生成さ
25 れるので、別人の個人情報から同一のユニークコードが生成される可能性が一段
と低くなり、一次変換データの有用性を、より一層高いレベルで保つことができ
る。

(5) 第5の発明によれば、第1の発明の情報管理装置において、二次変換データ生成手段により、一次変換データを暗号化して二次変換データを生成し、出力

手段によって二次変換データを他の装置へ出力し、出力手段により二次変換データが出力された際に、出力された二次変換データと、二次変換データのもとになった一次変換データと、一次変換データのもとになった処理対象のデータと、出力手段による出力記録とを対応づけて記憶手段に記憶する。従って、情報管理装置において、個人情報を含む処理対象のデータと、ユニークコードを含む一次変換データと、二次変換データと、二次変換データの送信記録とを、確実に保存しておくことができる。

(6) 第6の発明によれば、個人情報を含むデータを処理する情報管理装置と、情報管理装置により処理されたデータを管理する情報センタ装置とが通信回線を介して接続されてなる情報管理システムにおいて、情報管理装置は、個人情報抽出手段によって、処理対象のデータから個人情報を抽出し、ユニークコード生成手段により、個人情報抽出手段により抽出された個人情報をもとに一方関数を用いた演算を行ってユニークコードを生成し、一次変換データ生成手段により、処理対象のデータ中の個人情報をユニークコードに置き換えて一次変換データを生成し、二次変換データ生成手段により、一次変換データを暗号化して二次変換データを生成し、生成した二次変換データを、出力手段によって通信回線を介して情報管理装置に出力し、出力手段により二次変換データが出力された際に、出力された二次変換データと、この二次変換データのもとになった一次変換データと、この一次変換データのもとになった処理対象のデータと、出力手段による出力の記録とを対応づけて記憶手段に記憶する。また、情報センタ装置は、受信手段によって情報管理装置から送信された二次変換データを受信し、復号手段により、受信手段によって受信された二次変換データを復号して一次変換データを生成する。これにより、第1の発明により得られる効果に加えて、情報管理装置から情報センタ装置へ、一次変換データを暗号化して送信することによって、セキュリティ上の信頼性を確保することができる。そして、情報管理装置とは別の装置である情報センタ装置に、一次変換データのみを送信するので、情報センタ装置に情報を送信する間、および、情報センタ装置において情報を処理する過程において、個人情報が漏洩する可能性を無くすることができる。

(7) 第7の発明は、第6の発明の情報管理システムにおいて、情報センタ装置

は、復号手段により生成された一次変換データを格納するデータ格納手段をさらに備え、データ格納手段に格納されたデータを、ユニークコードをキーとして処理する。これにより、データ格納手段には、個人情報を含まない一次変換データが格納されたデータ格納手段を用いて各種の統計的な処理を行うことができる。

- 5 従って、個人情報を確実に保護しながら、個人情報を含むデータを用いた場合と同等の正確なデータ処理が行える。

(8) 第8の発明は、第7の発明の情報管理システムにおいて、情報センタ装置は、データ格納手段に格納された、ユニークコードを含む複数のデータの中から、同一のユニークコードを含むデータを検出する。すなわち、個人情報を含む複数の
10 のデータに対して個人情報をキーとして検出処理を行うのと同様に、個人情報を含まない複数の一次変換データに対して、ユニークコードをキーとして検索を行う。これにより、個人情報を用いることなく、同一人に係るデータと別の人に係るデータとを区別してデータを処理することが可能となる。

(9) 第9の発明によれば、上記第1の発明と同一の効果が得られる。

- 15 (10) 第10の発明によれば、上記第2の発明と同一の効果が得られる。

(11) 第11の発明によれば、上記第3の発明と同一の効果が得られる。

(12) 第12の発明によれば、上記第4の発明と同一の効果が得られる。

(13) 第13の発明によれば、上記第5の発明と同一の効果が得られる。

請求の範囲

1. 個人情報を含むデータを処理する情報管理装置であって、
処理対象のデータから個人情報を抽出する個人情報抽出手段と、
5 前記個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するユニークコード生成手段と、
前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成する一次変換データ生成手段と、
を備えることを特徴とする情報管理装置。
- 10 2. 前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータとを対応づけて記憶する記憶手段をさらに備えることを特徴とする請求項 1 記載の情報管理装置。
3. 前記ユニークコード生成手段は、前記個人情報抽出手段により抽出された個人情報から基準文字列を生成する基準文字列生成手段と、前記基準文字列をキー
15 として、所定の演算対象文字列を前記一方向関数により演算することによって、前記ユニークコードを生成する演算手段とを備えて構成されることを特徴とする請求項 1 記載の情報管理装置。
4. 前記演算手段は、前記基準文字列に基づいて演算桁数を決定する桁数決定手段と、前記演算桁数を有する演算対象文字列を生成する演算対象文字列生成手段
20 と、前記基準文字列をキーとして前記演算対象文字列を前記一方向関数により演算する演算実行手段とを備えて構成されることを特徴とする請求項 3 記載の情報管理装置。
5. 前記一次変換データを暗号化して二次変換データを生成する二次変換データ生成手段と、前記二次変換データを他の装置へ出力する出力手段と、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データ
25 と、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力記録とを対応づけて記憶する記憶手段と、をさらに備えることを特徴とする請求項 1 記載の情報管理装置。

6. 個人情報を含むデータを処理する情報管理装置と、前記情報管理装置により処理されたデータを管理する情報センタ装置とが通信回線を介して接続されてなる情報管理システムであって、

前記情報管理装置は、

- 5 処理対象のデータから個人情報を抽出する個人情報抽出手段と、
前記個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するユニークコード生成手段と、
前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成する一次変換データ生成手段と、
- 10 前記一次変換データを暗号化して二次変換データを生成する二次変換データ生成手段と、
前記二次変換データを、前記通信回線を介して前記情報管理装置に出力する出力手段と、
前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力の記録とを対応づけて記憶する記憶手段とを備え、
前記情報センタ装置は、前記情報管理装置から送信された二次変換データを受信する受信手段と、
- 20 前記受信手段により受信された二次変換データを復号して前記一次変換データを生成する復号手段とを備えること、を特徴とする情報管理システム。

7. 前記情報センタ装置は、前記復号手段により生成された一次変換データを格納するデータ格納手段をさらに備え、

- 25 前記データ格納手段に格納されたデータを、前記ユニークコードをキーとして処理することを特徴とする請求項6記載の情報管理システム。

8. 前記情報センタ装置は、前記データ格納手段に格納された、前記ユニークコードを含む複数のデータの中から、同一のユニークコードを含むデータを検出することを特徴とする請求項7記載の情報管理システム。

9. 個人情報を含むデータを処理する情報管理用コンピュータに、

個人情報抽出手段によって処理対象のデータから個人情報を抽出するステップと、ユニークコード生成手段により、前記個人情報抽出手段によって抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するステップと、

- 5 一次変換データ生成手段により、前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成するステップと、を含む処理を実行させるためのプログラム。

10 10. 前記情報管理用コンピュータに、前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータとを対応づけて記憶手段に記憶するステップをさらに含む処理を実行させることを特徴とする請求項9記載のプログラム。

15 11. 前記ユニークコード生成手段によりユニークコードを生成するステップは、前記個人情報抽出手段により抽出された個人情報から基準文字列生成手段によって基準文字列を生成するステップと、演算手段によって、前記基準文字列をキーとして所定の演算対象文字列を前記一方向関数により演算することにより前記ユニークコードを生成するステップとからなることを特徴とする請求項9記載のプログラム。

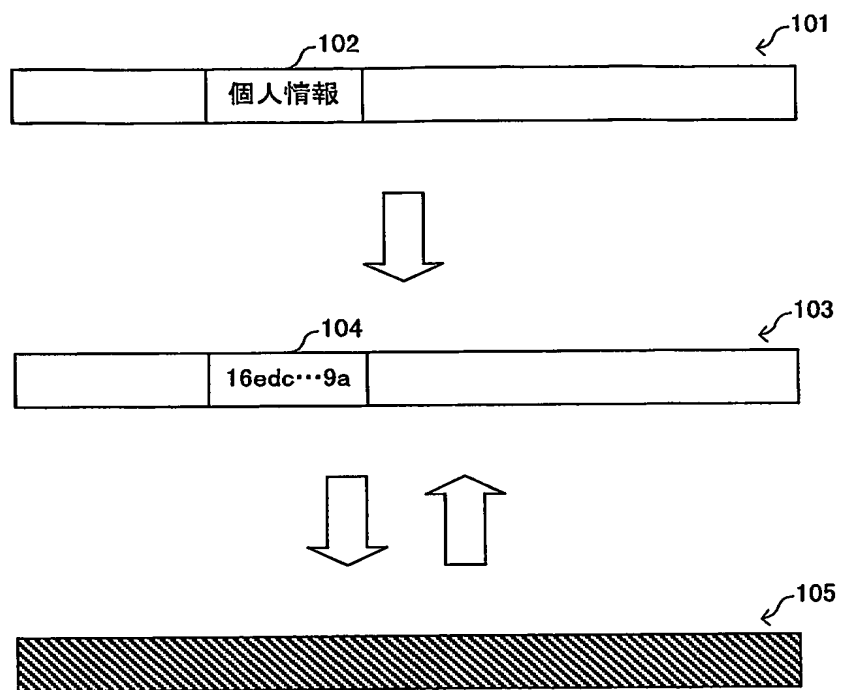
20 12. 前記演算手段によって前記ユニークコードを生成するステップは、桁数決定手段によって前記基準文字列に基づいて演算桁数を決定するステップと、演算対象文字列生成手段によって前記演算桁数を有する演算対象文字列を生成するステップと、演算実行手段により前記基準文字列をキーとして前記演算対象文字列を前記一方向関数により演算するステップとからなることを特徴とする請求項11記載のプログラム。

25 13. 前記情報管理用コンピュータに、二次変換データ生成手段によって前記一次変換データを暗号化して二次変換データを生成するステップと、出力手段によって前記二次変換データを他の装置へ出力するステップと、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力記録とを対応づけ

て記憶手段に記憶するステップとをさらに含む処理を実行させることを特徴とする請求項 9 記載のプログラム。

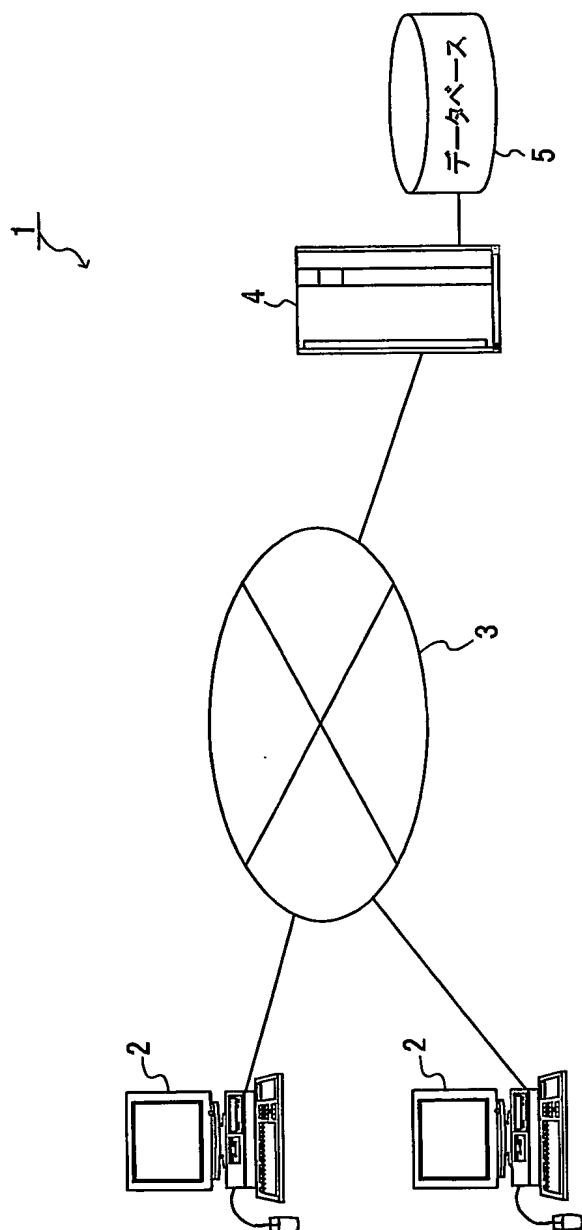
1/10

第1図

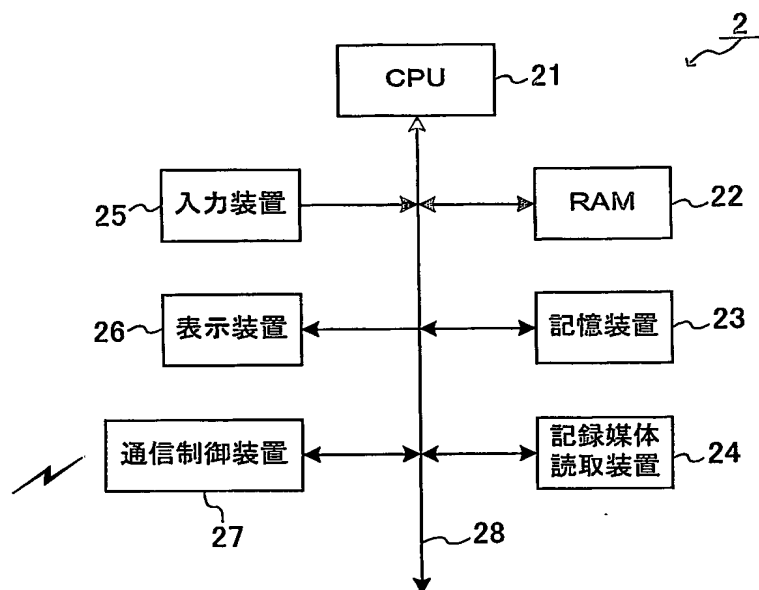


2/10

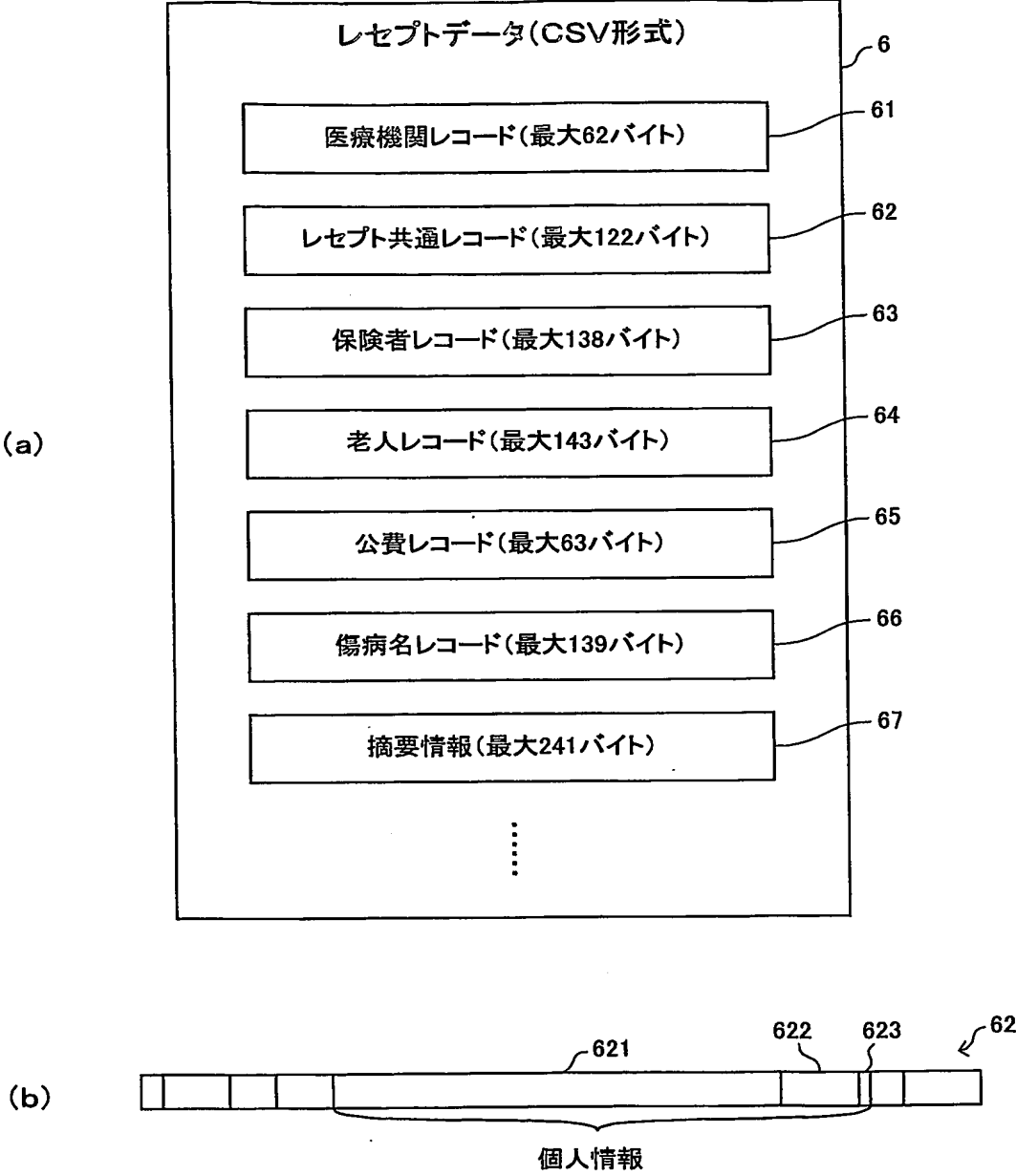
第2図



第3図

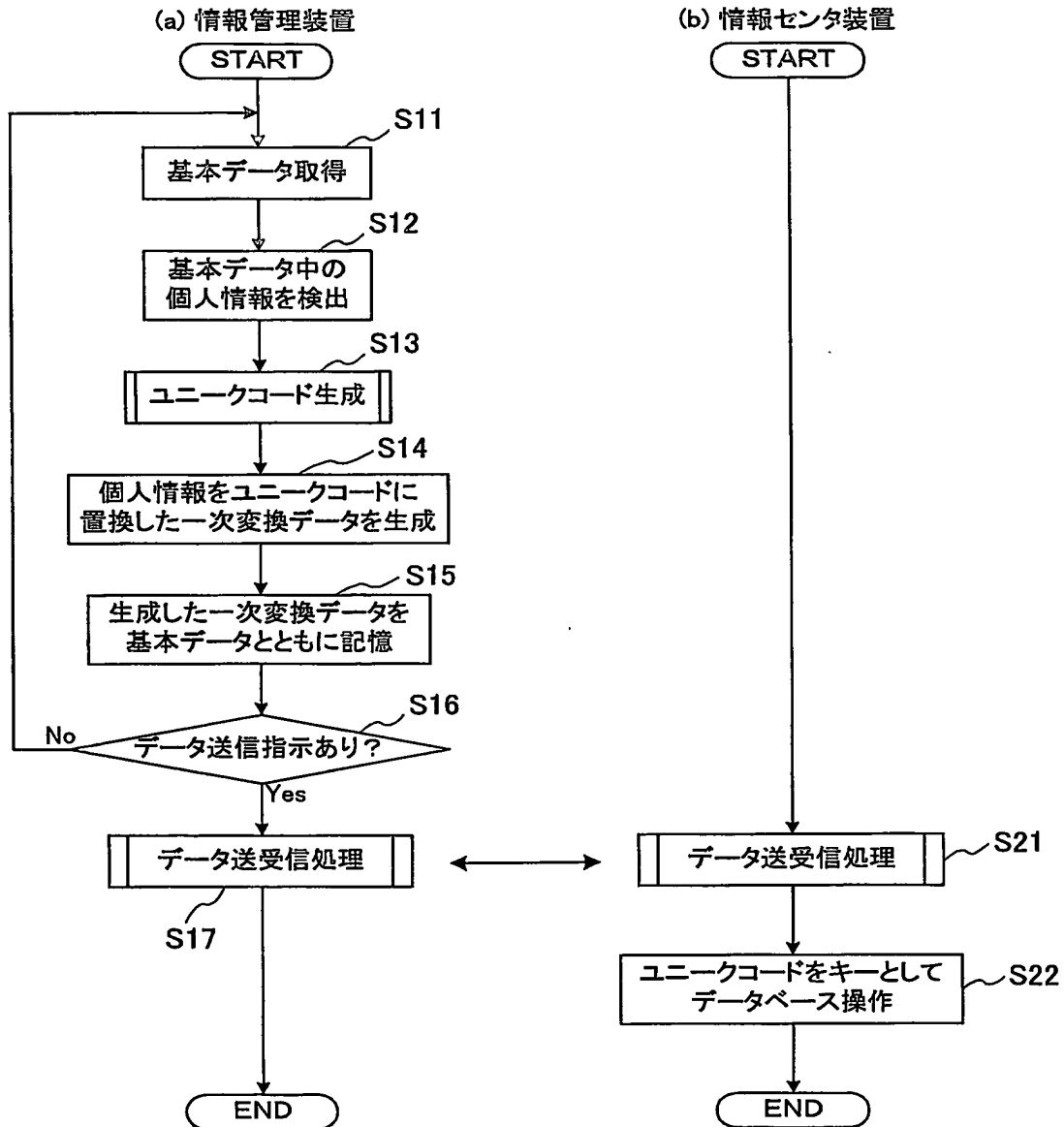


第4図



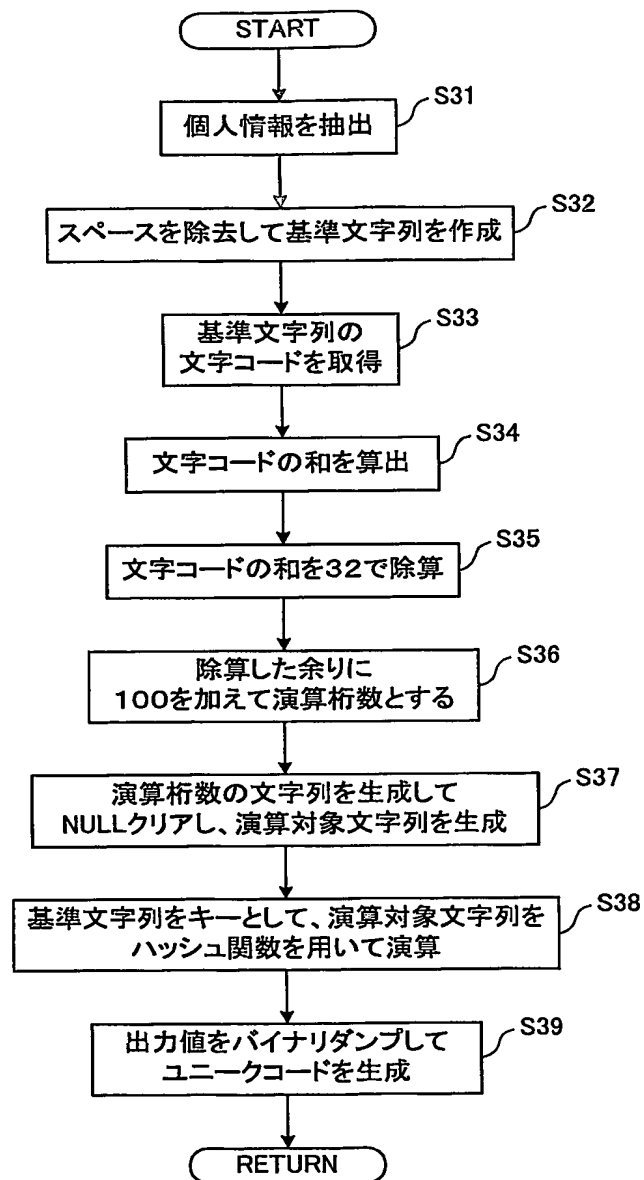
5/10

第5図



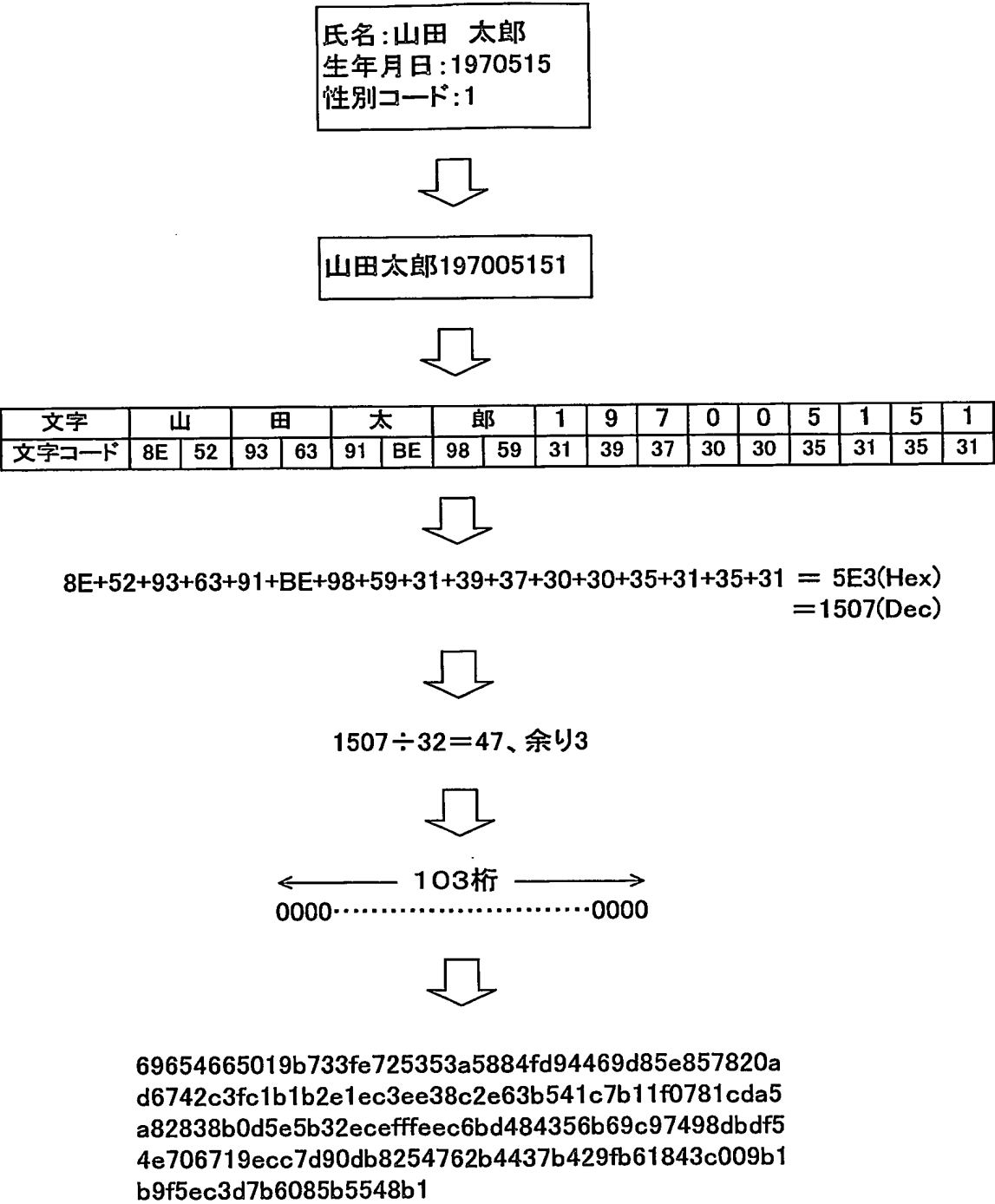
6/10

第6図



7/10

第7図



8/10

第8図

氏名:Nancy Lopez
 生年月日:1970226
 性別コード:2



NancyLopez197002262



文字	N	a	n	c	y	L	o	p	e	z
文字コード	4E	61	6E	63	79	52	6F	70	65	7A

文字	1	9	7	0	0	2	2	6	2
文字コード	31	39	37	30	30	32	32	36	32



$$4E+61+6E+63+79+52+6F+70+65+7A+31+39+37+30+30+32+32+36+32 = 5DB(\text{Hex}) \\ = 1499(\text{Dec})$$



$$1499 \div 32 = 46, \text{余り} 27$$



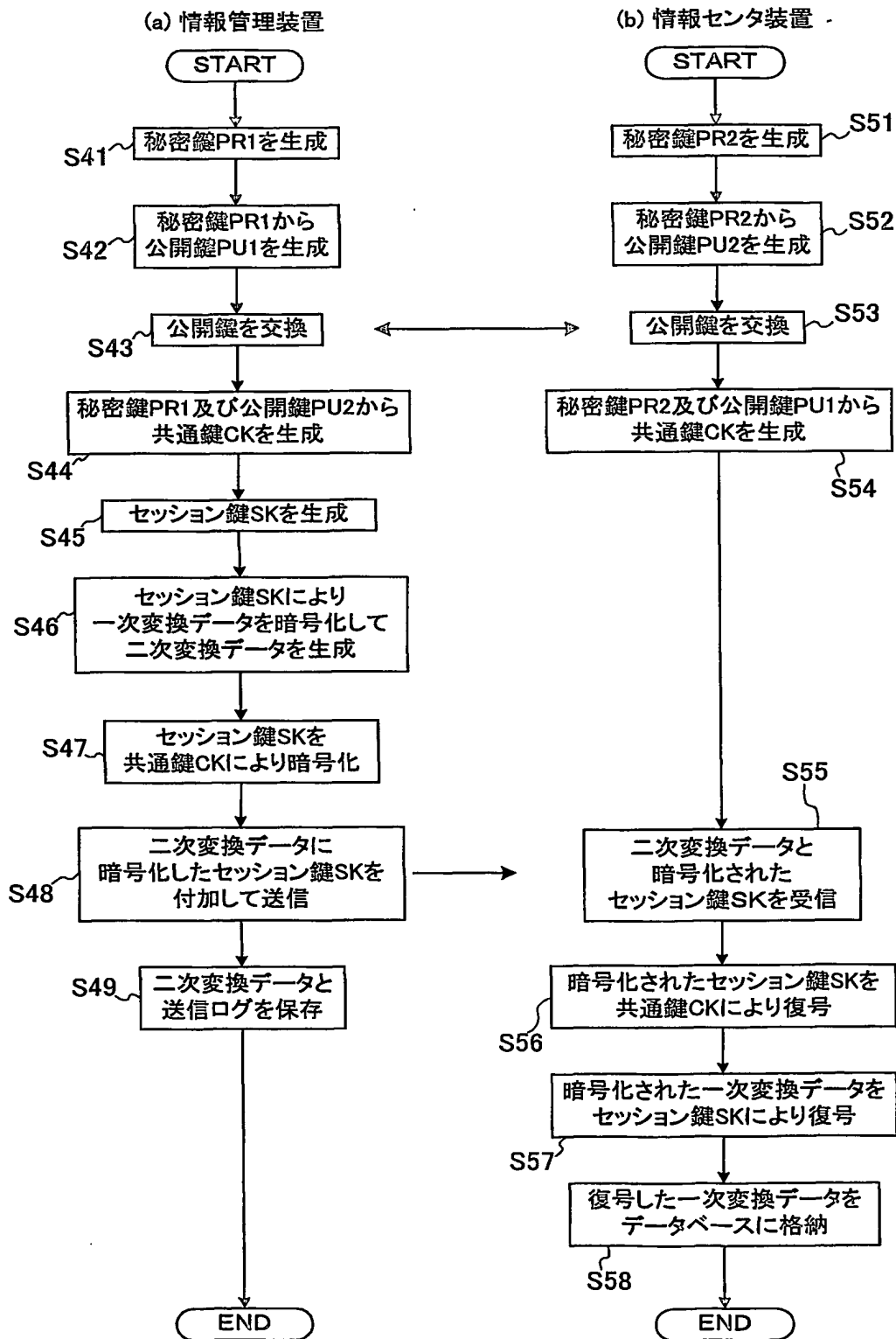
← 127桁 →
 0000.....0000



56b03813bad4c752a5c13247a0bc194ca607caf2e29564
 6a061027d09c00d9ec9767f6e825c521647b16a19df9ee
 6041ae400b7fa1026c93491d1d577a815129626493b6e9
 da791e85203fd00018e6022a0215afb571b67fffd47d3e68
 7dad79252ad98012bdd73d476edc0639a73cd9ca2a7f3c
 831e065bdd

9/10

第9図



10/10

第10図

No.	氏名	生年月日	性別	医療機関名	傷病名	診療日数	診療内容
1	山田太郎	19700515	1	〇〇〇	----	----	----
2	小泉次郎	19551120	1	〇〇〇	----	----	----
3	日本花子	19990101	2	〇〇〇	----	----	----
4	山田太郎	19700515	1	△△△	----	----	----
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

第11図

No.	ユニークコード	医療機関名	傷病名	診療日数	診療内容
1	548b1695d8e9a2b6085b5	〇〇〇	----	----	----
2	697473cd0029ca38c3	〇〇〇	----	----	----
3	4576edc003063c8381	〇〇〇	----	----	----
4	548b1695d8e9a2b6085b5	△△△	----	----	----
⋮	⋮	⋮	⋮	⋮	⋮

1	548b1695d8e9a2b6085b5	〇〇〇	----	----	----
4	548b1695d8e9a2b6085b5	△△△	----	----	----

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/03413

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/08, G09C1/00, G06F17/30, G06F17/60, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/08, G09C1/00, G06F17/30, G06F17/60, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2002-245164 A (Mitsubishi Electric Corp.), 30 August, 2002 (30.08.02), Full text (Family: none)	1, 2 3, 5-11, 13 4, 12
Y A	JP 2002-149497 A (NTT Advanced Technology Corp.), 24 May, 2002 (24.05.02), Full text (Family: none)	3, 5-11, 13 1, 2, 4, 12
Y	JP 2002-279062 A (Toshiba Corp.), 27 September, 2002 (27.09.02), Fig. 9 (Family: none)	3, 6, 9, 11

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 12 May, 2003 (12.05.03)	Date of mailing of the international search report 27 May, 2003 (27.05.03)
--	---

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/03413

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-259219 A (Kabushiki Kaisha Kurei Fisshu), 13 September, 2002 (13.09.02), Full text (Family: none)	3, 6, 9, 11
Y	JP 11-45304 A (Nippon Steel Corp.), 16 February, 1999 (16.02.99), Par. No. [0034] (Family: none)	5, 6, 13
A	JP 2002-109045 A (Medical Bank System Kabushiki Kaisha), 12 April, 2002 (12.04.02), Full text (Family: none)	1-13

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, G09C1/00, G06F17/30, G06F17/60,
G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, G09C1/00, G06F17/30, G06F17/60,
G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2003年
日本国登録実用新案公報	1994-2003年
日本国実用新案登録公報	1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y A	JP 2002-245164 A (三菱電機株式会社) 2002.08.30, 全文 (ファミリーなし)	1, 2 3, 5-11, 13 4, 12
Y A	JP 2002-149497 A (エヌ・ティ・ティ・アドバンステクノロジー株式会社) 2002.05.24, 全文 (ファミリーなし)	3, 5-11, 13 1, 2, 4, 12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

12.05.03

国際調査報告の発送日

27.05.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行



5M

9469

電話番号 03-3581-1101 内線 3598

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 2002-279062 A (株式会社東芝) 2002. 09. 27, 第9図 (ファミリーなし)	3, 6, 9, 11
Y	J P 2002-259219 A (株式会社クレイフィッシュ) 2002. 09. 13, 全文 (ファミリーなし)	3, 6, 9, 11
Y	J P 11-45304 A (新日本製鐵株式会社) 1999. 02. 16, 【0034】段落 (ファミリーなし)	5, 6, 13
A	J P 2002-109045 A (メディカルバンクシステム株式会社) 2002. 04. 12, 全文 (ファミリーなし)	1 - 13